SCOPE報告会
ネットワーク層

2020年3月11日　才所敏明
セキュアIoTプラットフォーム協議会
(株)IT企画

説明項目

１．本SCOPE-PJ概要、「ネットワーク層」の目的・目標

２．検討対象IoTシステム、SSDTF構想

３．SSDTFのMQTT上での実現方式

４．類似する研究とSSDTF/MQTTとの関係

５．ネットワーク層の今後の活動予定

自己紹介

1970年4月～1994年12月　東京芝浦電気（東芝）・情報システム部門
　東芝Gの技術部門・研究部門の
　　研究開発活動環境の整備・高度化を推進
1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門
　東芝Gのセキュリティ技術開発・事業支援活動を推進
2007年10月　(株)IT企画を設立
　情報技術および情報セキュリティ技術分野の研究開発や
　その応用事業に対するプロフェッショナルサービスを開始
［現職］　(株)IT企画　代表取締役社長
　事業支援活動：２社（日、米）（顧問・相談役）
　大学教育活動：九大、目白大　（情報セキュリティ）
　研究開発活動：中央大学研究開発機構、九州大学大学院、
　　セキュアIoTプラットフォーム協議会
　　暗号・認証、秘密分散、バイオメトリクス、電子メールセキュリティ
　　IoTシステムセキュリティ、FinTech（仮想通貨、ブロックチェーン）
　　ビッグデータ、AI

１．

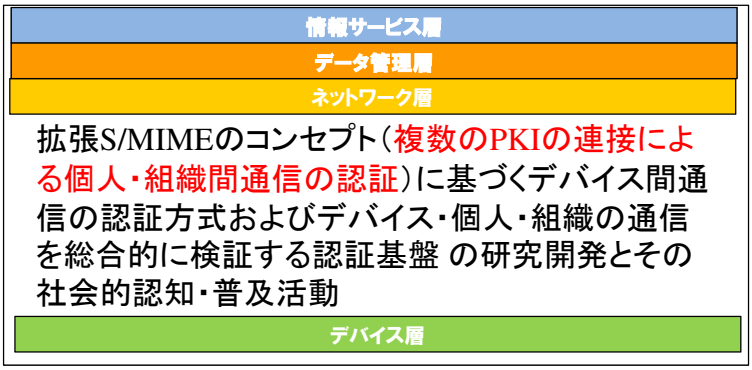
本SCOPE-PJ概要、「ネットワーク層」の目的・目標

IoTデバイス認証基盤の構築と新AI手法による表情認識の医療介護への応用（SCOPE：2018～2020）

本研究は、IoT・Big-Data・AIを支える情報セキュリティ基盤の構築を目指し、電子認証(真正性確認)を軸とした4階層（デバイス層、ネットワーク層、データ管理層、情報サービス層）に対し研究開発／ビジネスモデル構築／社会的普及／ガイドライン・標準化の作成を図る。

また情報サービス層における応用として、要介護者・患者などの医療介護現場に対し、電子認証によりセキュリティを担保したうえでの、リーマン幾何学を用いたAI技術による表情認識システムを確立することを目的とする。

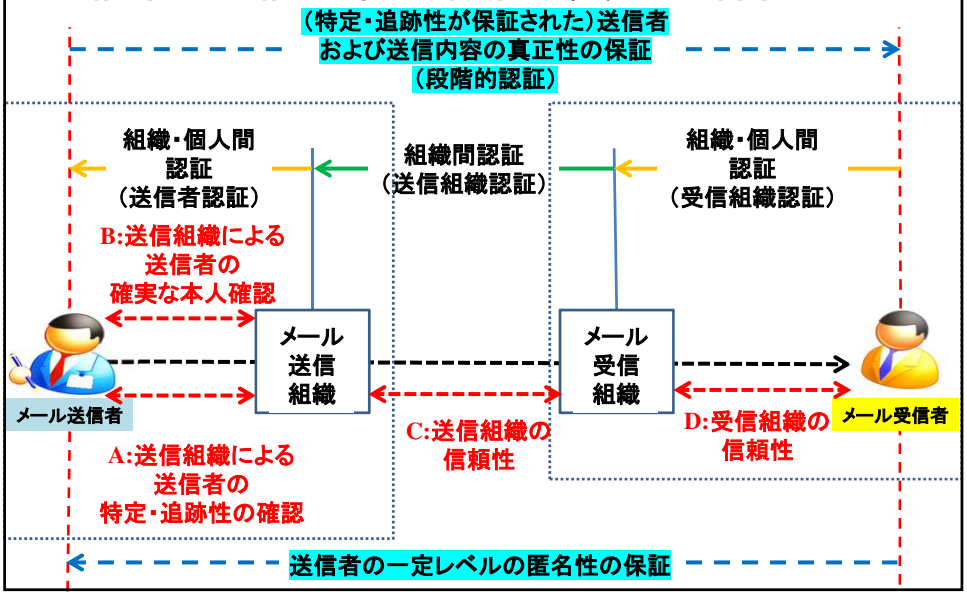
4階層から成る本PJにおける担当するネットワーク層の研究目的



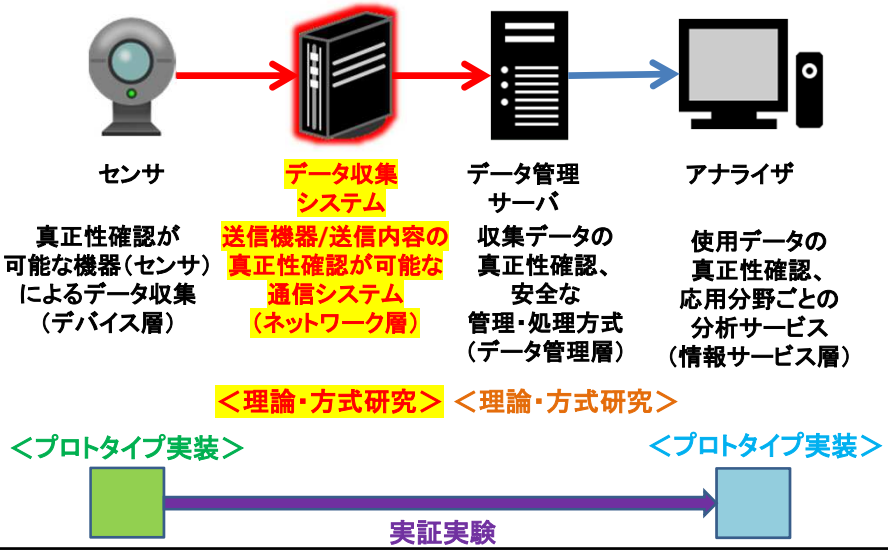
ネットワーク層の目標

IoTシステムにおける送信機器・送信内容の真正性確保のために、拡張S/MIMEのコンセプトに基づくIoTシステム向けの認証方式の提案およびその普及方策の策定を目標とする。

拡張S/MIME（SSMAX）における送信者・送信内容の認証（真正性保証）方式



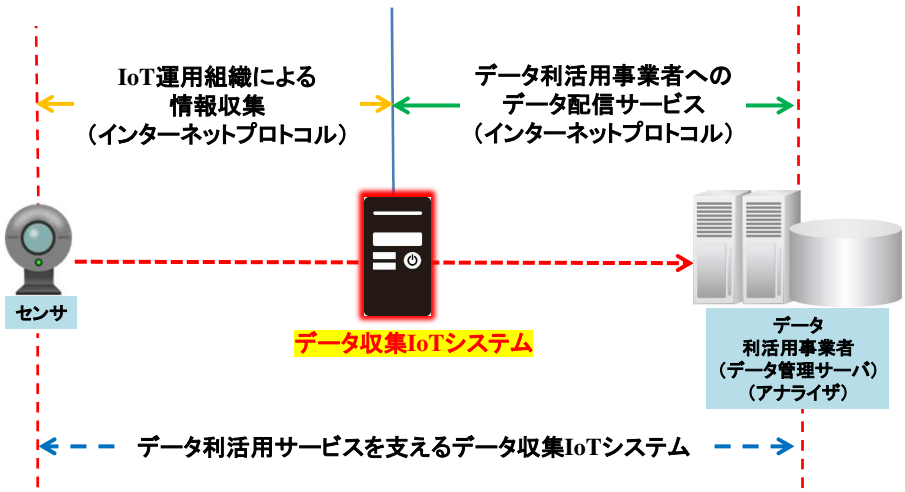
SCOPE研究開発課題の全体像と「ネットワーク層」の位置付け



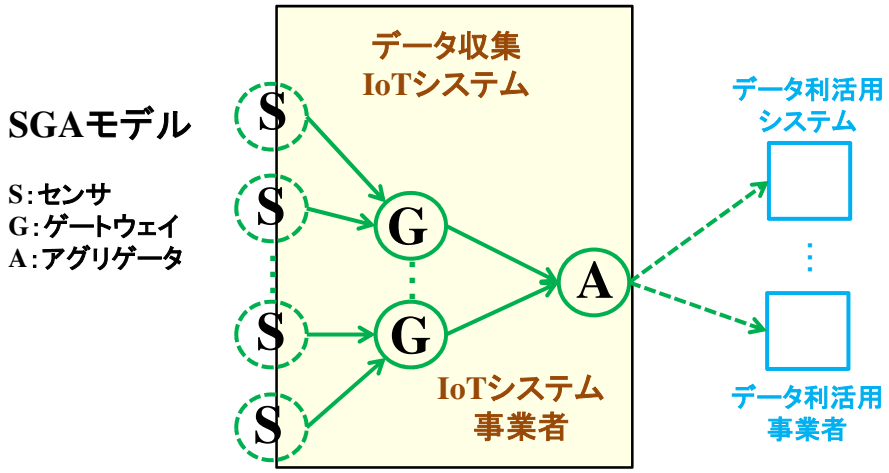
2.

検討対象IoTシステム、SSDTF構想概要

データ収集IoTサービスモデル/システム

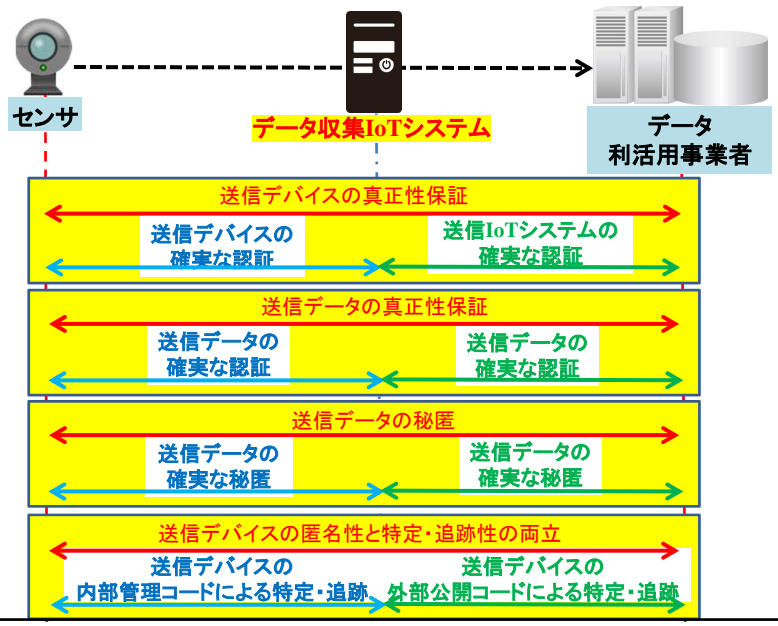


データ収集IoTシステムにおける ネットワーク層の具体的目標



➔SSMAXのコンセプトに基き、OSIのアプリケーション層上での SSDTF（Secure and Safe Data Transfer Framework）構想策定

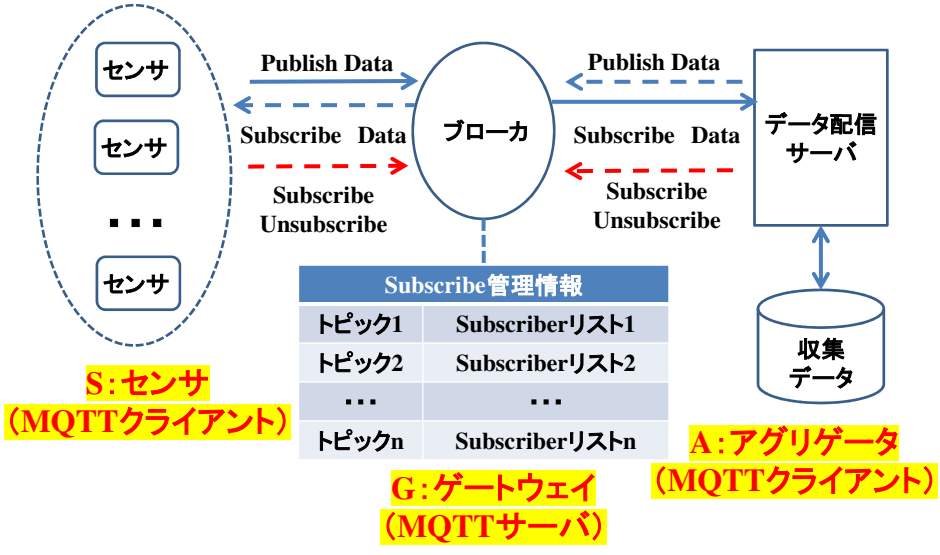
SSDTF構想で実現を目指す機能



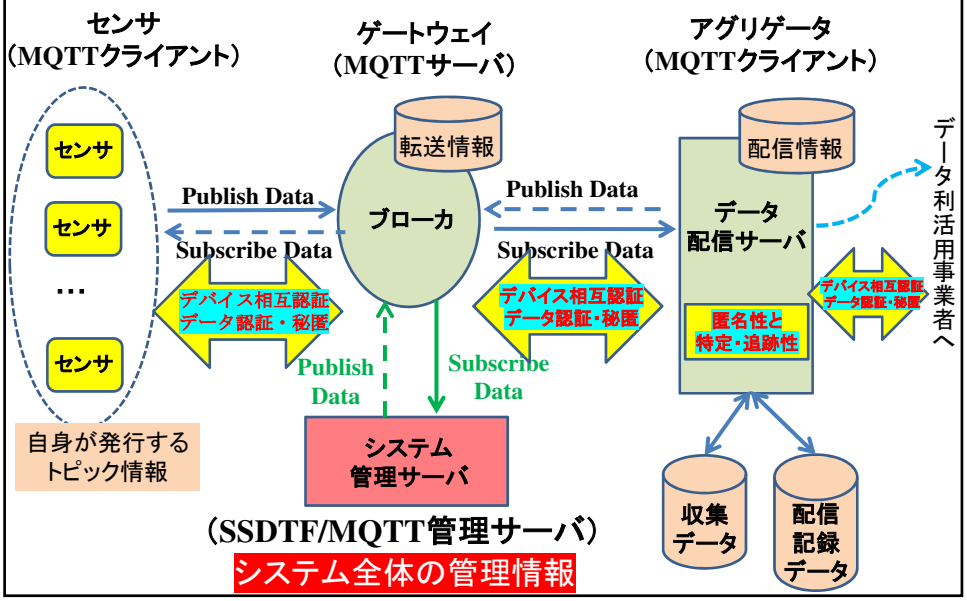
3.

SSDTFの MQTT上での実現方式

MQTTアーキテクチャとSGAモデルの対応付け



SSDTF/MQTT



SSDTF/MQTTで実現を目指す セキュリティ機能

(1)送信デバイスの真正性保証
　“公開鍵暗号、チャレンジ/レスポンス”による
　　送信・受信デバイスの真正性保証
(2)送信データの真正性保証
　“公開鍵暗号による署名付与・検証”による
　　送信データの真正性保証（非改ざん性保証）
　　送信デバイスの真正性保証
(3)送信データの秘匿
　“公開鍵暗号による暗号化、ブローカでは復号せずに再暗号化”による
　　送信データの漏洩防止
(4)送信デバイスの匿名性と特定・追跡性の両立
　“連結可能匿名化”による、
　　送信デバイスの内部IDの外部IDへの変換による匿名性保証
　　内部ID/外部ID対応表の管理による特定・追跡性保証

4.

類似する研究と SSDTF/MQTTとの関係

主要な類似研究論文一覧

①Secure MQTT for Internet of Things (IoT)

https://ieeexplore.ieee.org/document/7280018

②HOW TO AUTHENTICATE MQTT SESSIONS WITHOUT CHANNEL- AND BROKER SECURITY

https://arxiv.org/pdf/1904.00389.pdf

③Securing MQTT protocol in IoT by payload Encryption Technique & Digital Signature

https://www.researchgate.net/publication/335328286_Securing_MQTT_protocol_in_IoT_by_payload_Encryption_Technique_Digital_Signature

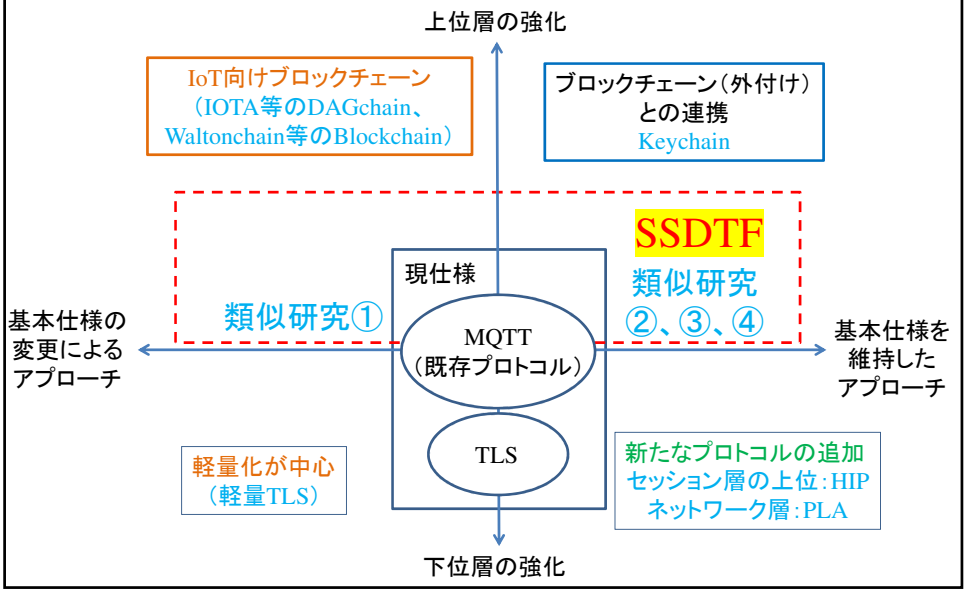
④LIGHTWEIGHT SECURE SCHEME FOR IOT-CLOUD CONVERGENCE BASED ON ELLIPTIC CURVE

http://www.jatit.org/volumes/Vol97No1/13Vol97No1.pdf

主要な類似研究論文の対象

	①	②	③	④	SSDTF
送信デバイスの真正性保証	―	送信デバイス認証	―	相互認証	相互認証
送信データの真正性保証	―	―	公開鍵暗号による署名	独自方式による真正性保証	公開鍵暗号による署名
送信データの秘匿	トピックの受信デバイス向け暗号化	―	ブローカによる復号・再暗号化	ブローカによる復号せず再暗号化	ブローカによる復号せず再暗号化
送信デバイスの匿名性と特定・追跡性の両立	―	―	―	―	連結可能匿名化

MQTTにおける セキュリティ強化策分類



5.

ネットワーク層の今後の活動予定

ネットワーク層の今後の活動予定

（1）SSDTF 構想のMQTT 上での具現化方式
SSDTF/MQTT の基本仕様策定

（2）関連研究の調査・分析による
SSDTF構想の独自性・特徴等の整理

（3）IoTデバイスおよび人が情報を発信する際の
認証の枠組みの総合的整理

謝辞

本研究は，総務省「戦略的情報通信研究開発推進事業SCOPE（受付番号：181603006）」にて、セキュアIoTプラットフォーム協議会及び中央大学のチームが採択を受けた「IoTデバイス認証基盤の構築と新AI手法による表情認識の医療介護への応用についての研究開発」の活動の一環として行ったものである。

終

（ご清聴、ありがとうございました。）

付録1

インターネットの現状に対する報告者の問題意識

インターネットの現状

＊日本のインターネットの歴史は1984年に始まり、
未だ35年余りだが、産業界の様々の活動、
国民の日々の生活に欠かせないものに。

＊TCP/IPが発表されインターネットという言葉がはじめて使われた
1974年当時は、インターネット利用者が他の利用者を
攻撃することは想定されていなかった。
➔ さまざまの攻撃、悪意の氾濫！

＊ICT技術の発展は留まるところを知らず、
社会はますますインターネットへ依存を強めるのは必至。
インターネット経由の様々の攻撃（悪意）もそれに応じ増大し、
社会の被害も甚大化することが想定される。
➔ インターネットのセキュリティ強化が不可欠！

 27

諸悪の根源は
インターネットの匿名性（特定・追跡困難性）

標的型攻撃メール/フィッシングメール→送信者の匿名性

誹謗・中傷・いじめ→発信者/発言者の匿名性

DOS/DDOS攻撃→攻撃サイト/乗っ取られた機器の匿名性

暗号通貨によるマネーロンダリング
→送金者/受領者の匿名性

➔現在のインターネットは
犯罪者（悪意のある人）に優しいシステム！

 28

インターネットの利用者認証の問題

On the Internet, nobody knows you're a dog

Cartoon written by Peter Steiner, published by The New Yorker on July 5, 1993

 29

研究の視点
安心・安全なインターネット社会に向けて

特定・追跡性の必要性

インターネットの悪用・不正利用を
安易に実行できない仕組みはもちろん、
万一の場合、悪用・不正利用者を容易に特定・追跡でき、
すみやかに止めることができる仕組みが必要

匿名性の重要性

利用者の特定・追跡情報の一般公開は以下の点で問題

＊プライバシー情報の無差別な拡散に繋がりかねない
＊自由な発言にブレーキ（インターネット活用にも？）の懸念も
＊コミュニティに応じた複数の人物を演じ楽しむ権利の剥奪

➔ インターネット利用者の確実な匿名性と特定・追跡性の両立が、
安心・安全なインターネット社会の実現に不可欠！

 30

Differential Traceability

ACMの2018年8月号にインターネットの父の一人
Vinton Gray Cerf氏の、”Traceability”の記事で提案された概念。

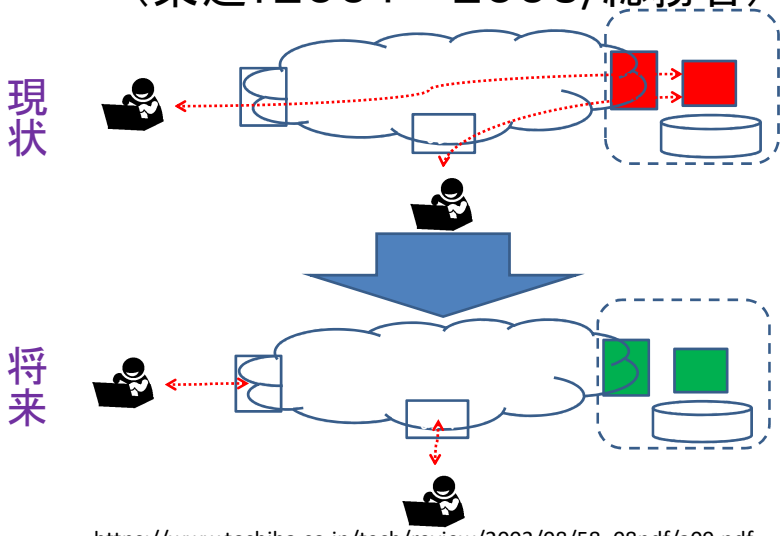
Vinton G. Cerf氏は、「Differential Traceability」の現実世界での簡単な例として、「自動車のナンバープレートに記載されている記号・番号には匿名性があるが、警察等の正式の要請により所有者情報が開示される」を提示し、インターネットの世界でも、同様の匿名性と特定・追跡性の両立が必要なのでは、という問題を提起したもの。

➔ ここ数年、インターネットの利用に関し報告者が主張してきた、
「特定・追跡性が保証されない匿名性は有害」
「匿名性と特定・追跡性の両立が不可欠」
に相通じる概念。
➔ 今後、国際の場でも議論が活発化することを期待。

付録2

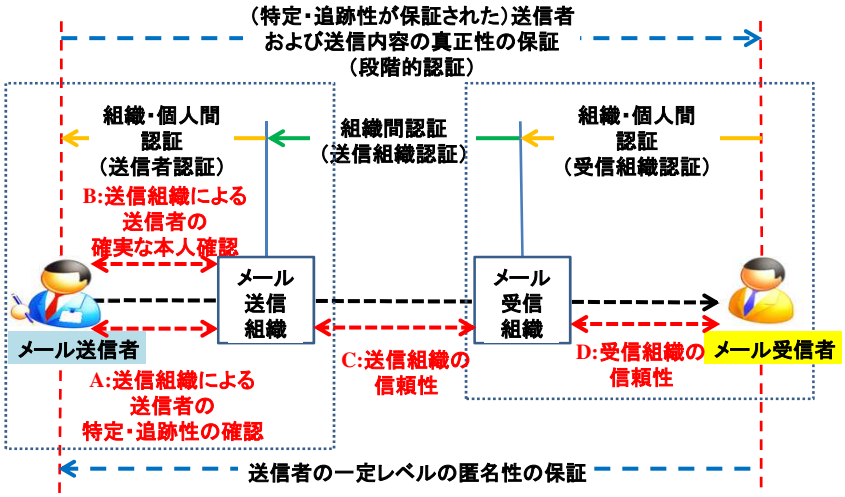
インターネットにおける匿名性と特定・追跡性の両立に関連する報告者の研究一覧

（1）出所不明のパケット流通を許さないセキュアな情報通信ネットワークの研究開発（東芝：2001～2003/総務省）

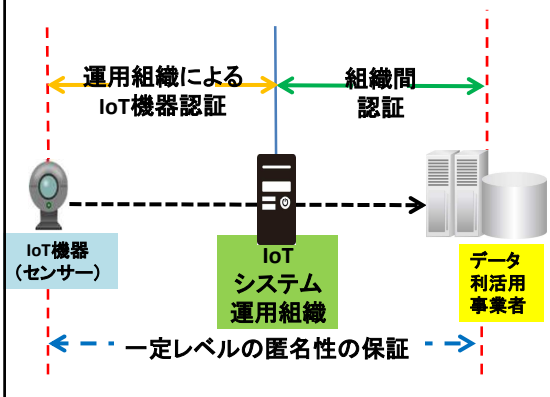


https://www.toshiba.co.jp/tech/review/2003/08/58_08pdf/a09.pdf

(2)拡張S/MIME(SSMAX)における送信者・送信内容の認証(真正性保証)方式 (IT企画:2016～2018/中央大学)



(3)安心・安全なIoTシステムフレームワーク SSIoT(Secure and Safe IoT System Framework) (IT企画:2017～2018中断中/中央大学)



階層	名称	活用想定技術
7	アプリケーション層	SSMAX (組織暗号、他)
6	プレゼンテーション層	
5	セッション層	HIP (Host Identity Protocol) PLA (Packet Level Authentication)
4	トランスポート層	
3	ネットワーク層	
2	データリンク層	
1	物理層	

特定・追跡性の必要性:
　被害拡大防止、早期正常化のための問題のあるデータ送信IoT機器への早期対応
匿名性の必要性:
　サイバー攻撃等のリスク低減のための物理的・論理的アドレス、その他の機微情報の秘匿

 35

(4)安心・安全な暗号資産システム (IT企画:2018～/九州大学)

悪用される暗号資産の現状

➔ 特定・追跡性が保証された匿名性のある暗号資産が必要！

暗号資産の匿名性に関する調査・研究成果の発表

2019年1月25日　SCIS2019

仮想通貨の匿名性の現状と課題

2019年3月16日　IPSJ第81回全国大会

暗号仮想通貨における匿名化技術の現状と展望

2019年10月22日　CSS2019

匿名暗号資産(Monero/Zcash/Grin)
ブロックチェーンの匿名性に関する考察

2020年1月31日　SCIS2020

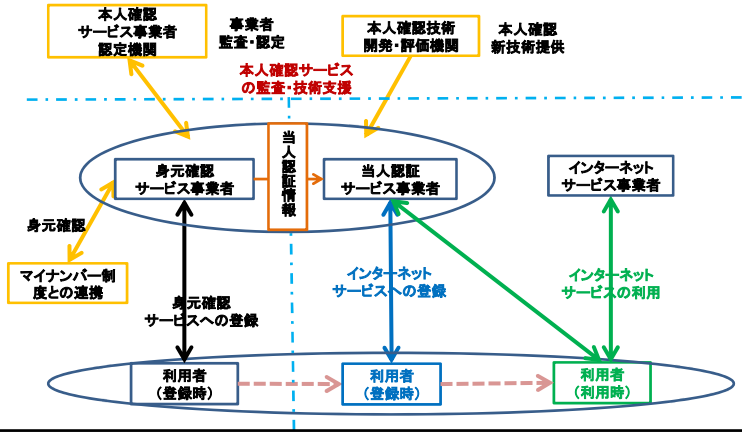
DAG技術ベースの暗号資産の匿名性に関する考察

 36

(5)匿名性と特定・追跡性の両立が可能な本人確認基盤 (IT企画:2018～)

安心・安全なインターネット社会実現には
利用者の特定・追跡性と同時に匿名性が保証された
本人確認基盤の構築・運用が必要

➔ NAFJP : National Authentication Framework in Japan の提案



終

（配布資料　最終ページ）